



Impact of Sarbanes-Oxley (SOX)

Presented by:
(301) 529-8118



Objectives

- General overview/update of the Sarbanes-Oxley (SOX) Act.
- Summary of the PCAOB guidelines issued in March.
- Impact of SOX on non-public companies and not-for-profits.
- Linkage of SOX to COSO framework



Why Are We Here - SOX?

- Enron
- Worldcom
- Adelphia
- Health South
- Etc.

What went wrong?

One Hundred Seventh Congress
of the
United States of America

AT THE SECOND SESSION

*Begun and held at the City of Washington on Wednesday,
the twenty-third day of January, two thousand and two*

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures
made pursuant to the securities laws, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Sarbanes-Oxley Act of 2002”.

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Commission rules and enforcement.

TITLE I—PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD



Impact of SOX

- New focus on controls, especially IT
- Lots of money being spent – but still may not be asking the right questions – IT'S NOT THE PROCESSES!
- It's about senior management!
- Lots of new software vendors
- Lots of revenue for smaller CPA firms
- Other regulators and countries will follow



SOX Targets

- **Public Accountants**
 - Oversight – PCAOB
 - Registration
 - Prohibited services
 - Documentation of work
 - Reviews of work – internal and external



SOX Targets

- **Board of Directors/Audit Committee**
 - Composition – Independence
 - Mandatory Audit Committees
 - Public Accounting Firm Oversight, Financial Experts, Resources, etc.
 - Whistle-blowing provisions



SOX Targets

- **Corporate Management**
 - Off-balance Sheet Transactions
 - Management Assessment of Internal Control (404)
 - CEO/CFO Certifications (302)
 - Penalties
 - Code of Ethics Required



SOX 302/404

- **302 CEO/CFO certifications**
 - No material financial misstatements
 - Designed internal controls would alert them ...
 - ...have evaluated internal controls
 - ...presented their conclusions about the effectiveness of internal controls
 - ... disclosed ...any significant deficiencies/or material weaknesses... as well as fraud...
 - ...reported any significant changes



SOX 302/404

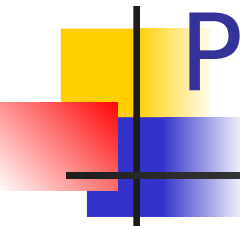
- **404 requires that annual reports contain:**
 - A statement that management is responsible for maintaining an adequate internal control structure and procedures for financial reporting
 - An assessment, as of the end of the most recent fiscal year, of the effectiveness of the internal control structure and procedures for financial reporting
 - Attestation of this assessment by the external audit firm



SOX 302/404

- **302 versus 404:**

- 302 certifications – controls over the timely, accurate, and complete disclosure of material non-financial information
- 404 assertions – controls over the integrity of financial reporting – including the safeguarding of assets



PCAOB Audit Guide

An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements

- Evaluate the process management uses to perform its assessment of internal-control effectiveness.
- Obtain an understanding of how the internal controls over financial reporting are designed and operate.
- Evaluate the effectiveness of the design of internal controls.
- Test the operating effectiveness of internal controls.
- Form an opinion about whether internal control over financial reporting is effective.



Peek-A-Boo!

- Can an organization called Peek-A-Boo really be taken seriously?
- Big 8, Big 6, Final 4, ???

PCAOB

Public Company Accounting Oversight Board

OH



Framework Used by Management

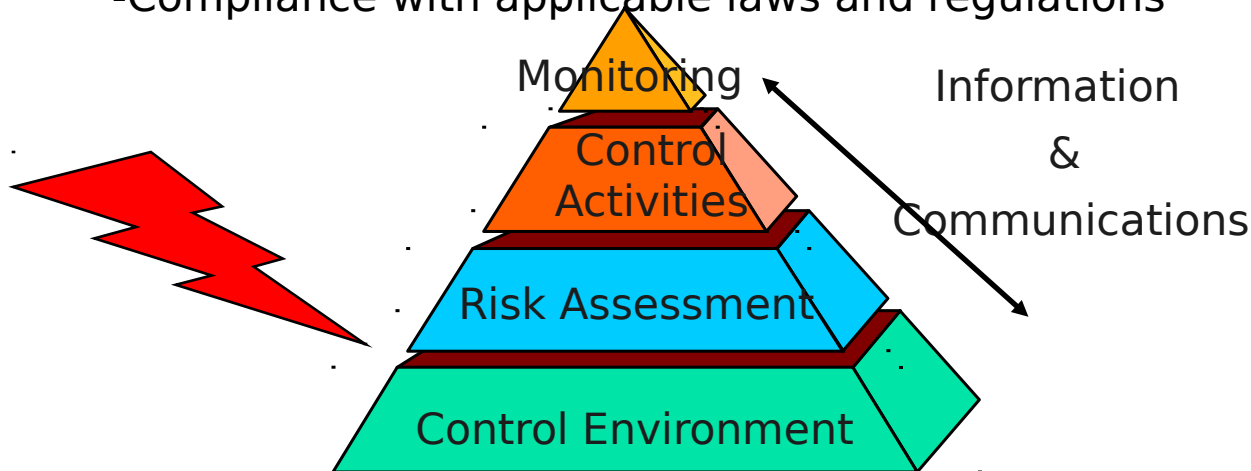
Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures, including the broad distribution of the framework for public comment. In addition to being available to users of management's reports, a framework is suitable only when it:

- Is free from bias;
- Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting;
- Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted; and
- Is relevant to an evaluation of internal control over financial reporting.

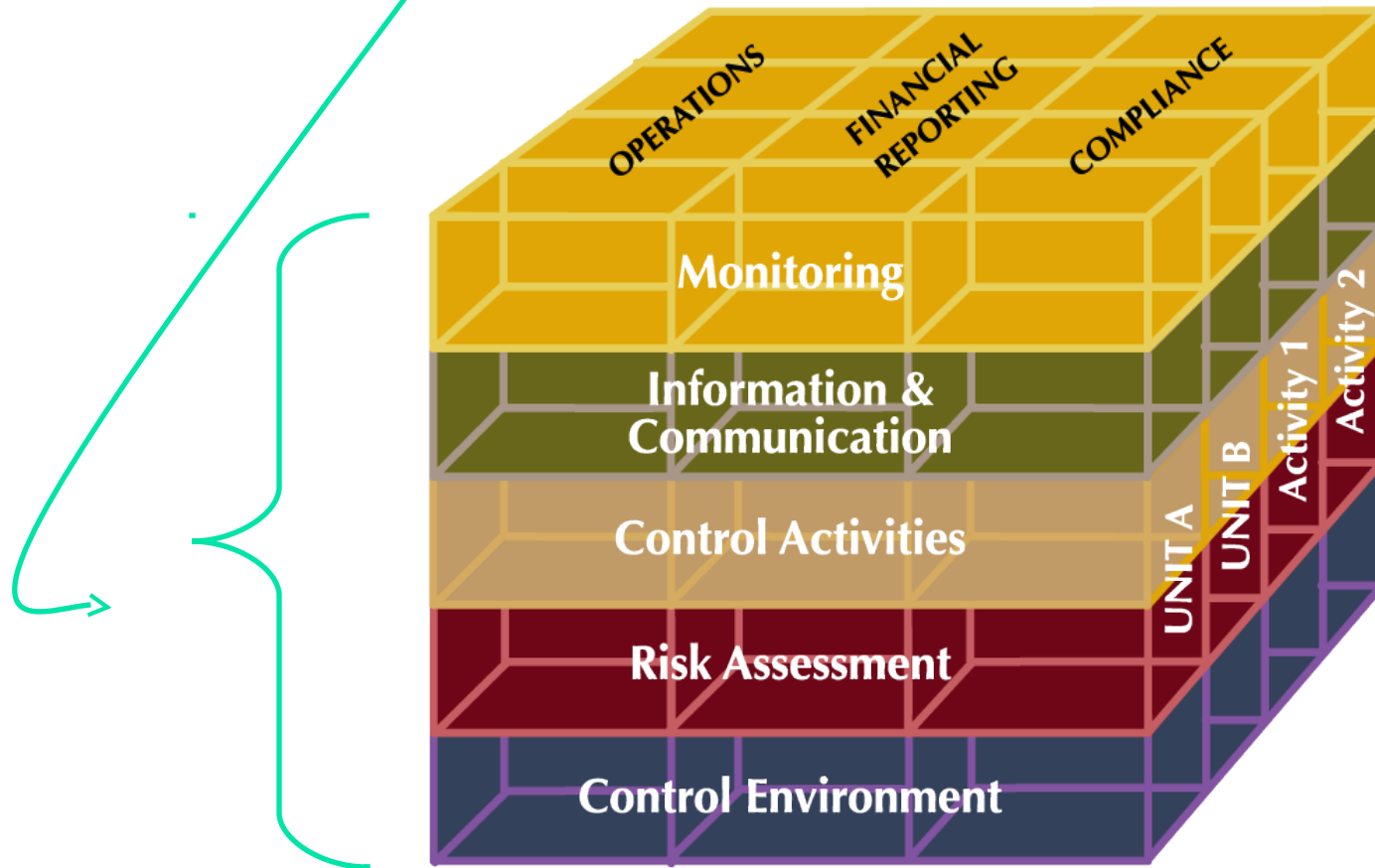
COSO Model of Control

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations



You Need COSO More Than SOX





Use a COSO Approach to SOX

404

- Consider the environment
- Identify financial reporting assertions – and worry about the “things that got us here” – risk assessment
- Controls in routine, non-routine and estimate data flows
- Information and Communication
- Monitoring

SOX 302/404 Flow

Management of company

Need agreement up front!!

Public accountants

Financials and disclosures

ID significant accounts, processes, locations

Document controls
Test controls
Assess controls

- Review control assessment process
- Review financial controls
- Test controls
- Opine on both financial controls and assessment process
- Opine on financials

This is where you think about “what got us here”

COSO - Entity level

- Control Environment
- Risk Assessment
- Info & Communications
- Monitoring

COSO - Activity level

- Risk Assessment
- Control Activities
- Info & Communications
- Monitoring



Agreement On:

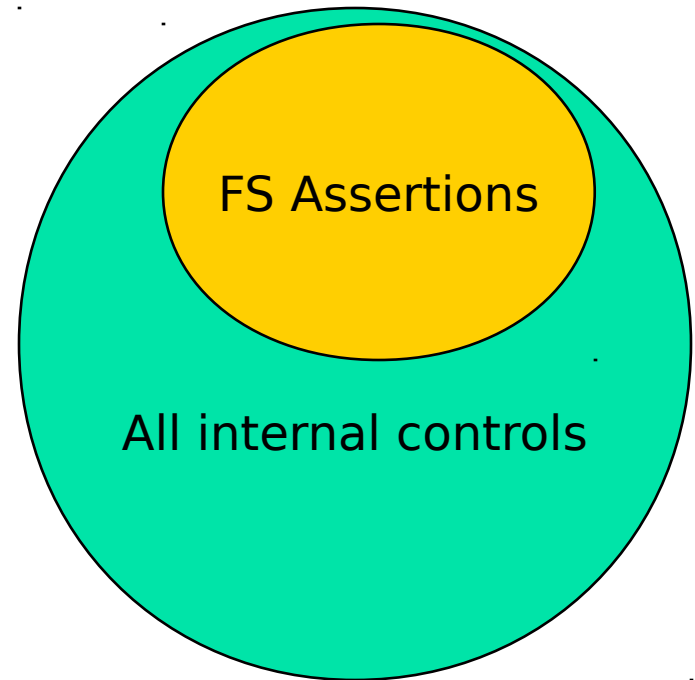
- Significant accounts
- Significant activities
- Where the risks – to financial statement accuracy - are
- Approach and software for documenting routine data flows – CAATS, RCM, flowcharts, etc.

Financial Statement Assertions

- Existence or occurrence
- Completeness
- Rights and obligations
- Valuation or allocation
- Presentation and disclosure

From COSO - Risk Assessment and
from SAS 31 - Evidential Matter

“Focus on Financial Statement
Assertions, not Significant
Controls” PCABO

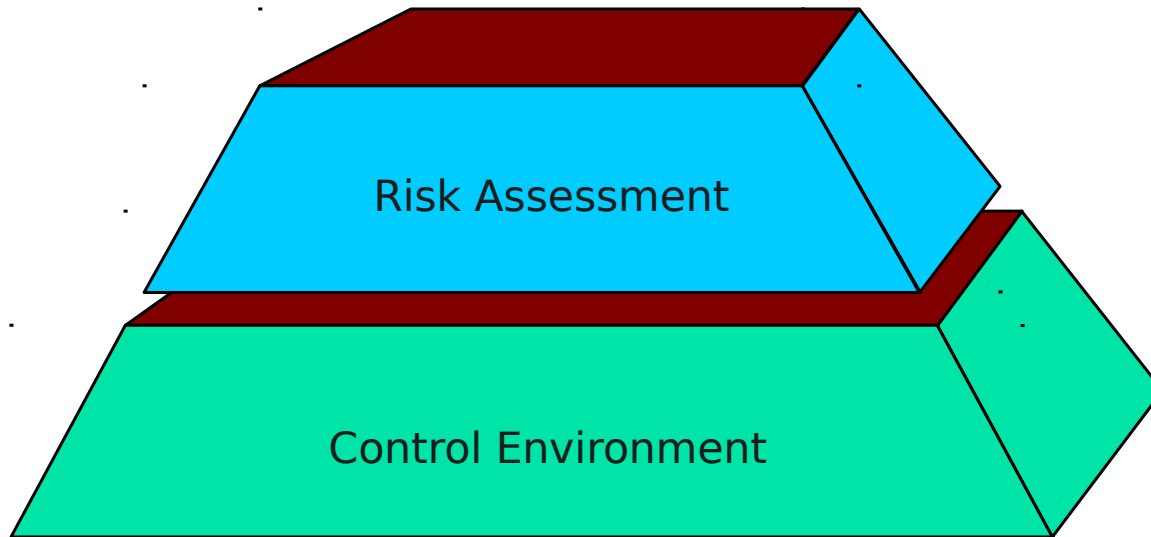




Another View of COSO



Environment and Risks





But How Do You Find It?

- Not the routine data flows
- Not by an inexperienced auditor
- Not by asking the senior executives



“Constructively Challenging” Questions

- Ask management:
 - “How do you know” that employees understand and practice our corporate values?”
 - “How do you know” the financials and disclosures are right?
- Ask employees:
 - “Do **other** employees in your area practice our corporate values?”
 - “Do you know where and how to report violations?”
 - “How do you feel” about management’s commitment to getting the financials and disclosures right?

You can’t find control environment problems by asking the ones that create the control environment



Tone at the Top

- "You'll see people who in the early days ... took their life savings and trusted this company with their money. And I have an awesome responsibility to those people to make sure that they're done right." - Bernard Ebbers
- "Most of us made it to the chief executive position because of a particularly high degree of responsibility.... We are offended most by the perception that we would waste the resources of a company that is a major part of our life and livelihood, and that we would be happy with directors who would permit that waste.... So as a CEO I want a strong, competent board." - Dennis Kozlowski
- "It's more than just money. You've got to give back to the community that supported you." - John Rigas

<http://www.thecorporatelibrary.com/spotlight/scandals/scandal-quicksheet.html>



Three Traits ...

... Fraudulent Corporations Had In Common

- Never grew up
- Immense greed labeled as entitlement
- Slaves to Wall Street

It's too much to say we should have seen this coming. But learning is a process of recognizing patterns, and we'll have no excuse if we fail to spot the next company that fits this one.

Geoffrey Colvin, *Fortune Magazine*



This is Not Rocket Science ...

- Off balance sheet entities
- Consolidating eliminations and reclassifications
- Post closing entries
- Last minute changes
- Looking for credits – revenue
- Estimations and reserves
- Related party transactions
- Loans and transactions with executives



Nor is it New Stuff ...

- Critical importance of tone at the top
- Importance of control environment, codes of conduct, involved audit committees, objective internal audit function
- Called for management to report on effectiveness of internal controls

*From Report of the National Commission on
Fraudulent Financial Reporting - 1987*



Other Thoughts

- Most of SOX is linkage, not creation of new stuff – except documentation
- RCM in COSO Evaluation Tools is only an example
- To ORCA, or to OCRRA
- COSO should be done by management, not the auditors



Risk – A Four Letter Word

- What is the risk to the company?
- Minimize the risk in your portfolio.
- What are the risks to achieving this objective?
- Risk-based auditing
- Risk Assessment component of COSO
- Risk Assessment to select audits to perform

Control Activities



If we can just be sure
of the basics ...

Think routine, non-routine
and estimation data flows



Are Inputs, Processing and Outputs ...

- Complete
- Authorized
- Accurate
- Timely
- Safeguarded

You can't ignore the computer – that's where all the routine data flows are controlled

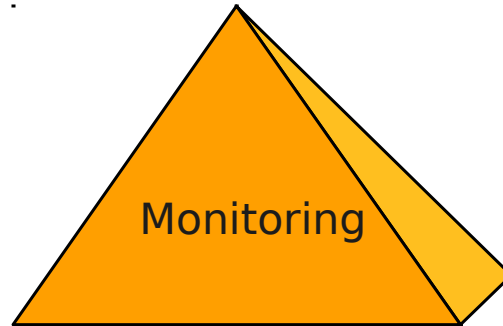
From Auditing 101



Information and Communication

- Would employees be able to surface a financial reporting or disclosure problem if they knew about one?
- How freely does bad information about financial results flow in the organization?

Controller



- NOUN: **1.** One that controls: *a controller, not an observer of events.* An officer who audits accounts and supervises the financial affairs of a corporation or of a governmental body. **2.** A regulating mechanism, as in a vehicle or electric device.

From the American Heritage® Dictionary of the English Language: Fourth Edition. 2000

- You can't monitor an organization into shape



Testing Controls

- Testing means gather audit evidence (sufficient, competent, relevant, useful)
- Testing soft controls is different than testing hard controls
- Most hard controls are I/T based!



It's Not Just Financial

Where are disclosure problems
likely to be found?

- In the operations
- In earnings meetings
- In budget reviews
- In profit planning

Accountants are the last to know



And COSO is NOT Just Financial!

- Where do you really need to meet objectives?
- Earnings is an operational thing, not a financial reporting thing.
- Where are the real risks to a company?
- Not in financial reporting – **it's the business!**



Don't Do SOX – Add Value!

Which is better?

Comply with the law

OR

Improve E&E of
financial reporting and disclosures



Impact on Not-for-Profits

- A permanent change in what a financial statement audit is
- Auditing internal controls and financials will become the standard audit process
- Will be expected of good companies
- IIA's Impact of SOX on Non-Public Audit Committees



Finding Fraud

- *Proactively Detecting Occupational Fraud Using Computer Audit Reports*

By: Richard B. Lanza, CPA, PMP

Foreword By: Joseph T. Wells, CFE, CPA Founder
and Chairman, Association of Certified Fraud
Examiners

An IIA Research Foundation Report



SAS 99

- *Increased emphasis on professional skepticism.* The audit team needs to set aside existing beliefs about management's honesty and exchange ideas on how frauds could occur.
- *Discussions with management.* The engagement team should ask management and others in the organization about the risk of fraud and whether they are aware of any frauds. The auditors should make a point of talking to employees in and outside management, thereby giving employees and others the opportunity and encouragement to "blow the whistle."
- *Unpredictable audit tests.* The engagement team should test areas, locations, and accounts that otherwise might not be tested. From the client's viewpoint, the tests should be unpredictable and unexpected.
- *Responding to management override of controls.* The standard includes procedures to test for management override of controls on every audit.



IA Responsibilities

- Have sufficient knowledge of fraud to be able to identify indicators that fraud may have been committed. This knowledge includes the need to know the characteristics of fraud, the techniques used to commit fraud, and the types of frauds associated with the activities reviewed.
- Be alert to opportunities, such as control weaknesses, that could allow fraud. If significant control weaknesses are detected, additional tests conducted by internal auditors should include tests directed toward identification of other indicators of fraud. Some examples of indicators are unauthorized transactions, override of controls, unexplained pricing exceptions, and unusually large product losses. Internal auditors should recognize that the presence of more than one indicator at any one time increases the probability that fraud may have occurred.

From Practice Advisory 1210.A2-1: Identification of Fraud



Think About The Future

- This is a PERMANENT CHANGE!
- SOX will happen year after year
- Integrate SOX data with IA data – single repository
- For internal auditors:
 - Ask the BOD what IA should be doing
 - Consult at your own risk ... the basics better be right first
 - Change your IA plan, but don't forget where the real risks are.



SOX is ...

- A time for clarity and agreement, at the front-end, with external accountants
- A time for management to take responsibility for internal controls
- A time for internal auditors to clarify their audit charters



Some References

- <http://www.thecorporatelibrary.com/spotlight/scandals/scandal-quicksheet.html>
- Proactively Detecting Occupational Fraud Using Computer Audit Reports, The IIA Research Foundation.
www.TheIIA.org
- Web sites of Big 4: EY, PWC, D&T, KPMG
- www.Knowledgeleader.com
- www.protiviti.com
- www.AICPA.org
- www.PCAOBUS.org
- www.ISACA.org for COBIT/SOX objectives
- Do a search using: worldcom enron adelphia healthsouth